

日 本 国 特 許 庁
JAPAN PATENT OFFICE

27. 1. 2004

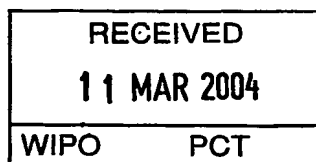
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 1月27日

出 願 番 号
Application Number: 特願2003-017637
[ST. 10/C]: [JP2003-017637]

出 願 人
Applicant(s): 松下電器産業株式会社

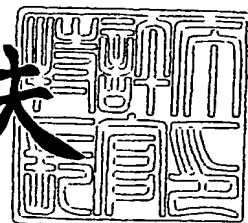


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 2月26日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 2032750008

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 三浦 康史

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 徳田 克己

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100109210

 【弁理士】

 【氏名又は名称】 新居 広守

【手数料の表示】

 【予納台帳番号】 049515

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 0213583

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルコンテンツ配信システム

【特許請求の範囲】

【請求項 1】 ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、

前記サーバ装置および前記端末装置間の通信に、少なくとも前記サーバ装置による前記端末装置の正当性の認証と通信暗号鍵の共有を行う認証フェーズを含み、

前記認証フェーズには、前記サーバ装置と前記端末装置間で通信されるトランザクションを識別する情報を交換するトランザクション識別情報交換フェーズと、前記トランザクションにおける前記端末装置からの先頭のコマンドを送信する先頭コマンド送信フェーズとを含むことにより、ユーザに対する応答時間を削減する

ことを特徴とするデジタルコンテンツ配信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを用いて、サーバ装置から映像、音楽などのデジタルコンテンツと、デジタルコンテンツの利用を許諾するライセンスを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、前記サーバ装置と前記端末装置間の通信において、不正にライセンスの複製や改ざんが行われることを防ぎつつ、通信切断発生時においてもライセンスの消失や二重配信をも防ぐシステムおよび装置に関する。

【0002】

【従来の技術】

近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテンツと記述）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末

装置に配信し、端末装置においてコンテンツを利用することが可能な、コンテンツ配信システムと呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術等を用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。

【0003】

例えば、特許文献1には、コンテンツ配信システムの一例として、暗号化されたコンテンツ、利用条件、および、コンテンツ復号鍵を端末装置が、サーバ装置より受信し、改ざん検出を行った後、利用条件の適合検証を行い、すべての検証を満足したときのみコンテンツの復号を行い出力するシステムが記載されている。

【0004】

このように、従来のコンテンツ配信システムでは、サーバ装置からライセンス（利用条件とコンテンツ復号鍵の総称。利用権利とも呼ぶ）を端末装置に配信するが、その配信経路は一般的にインターネットなどの公衆回線を用いるため、ライセンスの盗聴および改ざんを防ぐ必要がある。つまり、利用条件の不正改ざんやコンテンツ鍵の流出を防止しなければならない。さらに、サーバ装置はライセンス配信先の認証も行う必要がある。つまり、サーバ装置が意図しない端末装置にライセンスを配信することも防止する必要がある。盗聴・改ざん防止と通信相手の認証を行うプロトコルはSAC（Secure Authenticate Channel）プロトコルと呼ばれ、例えば、SSL（Secure Socket Layer）がよく知られている（非特許文献1）。

【0005】

また、通信装置・通信回線の故障や電源断などによる通信切断がライセンス配信中に発生した場合、そのライセンスが消失してしまう可能性がある。このような場合、購入したコンテンツを再生することができないといった不利益がユーザに発生する。例えば、特許文献2には、通信切断による通信データの消失を、デ

ータ再送によって回避するプロトコルが記載されている。

【0006】

【特許文献1】

特開平7-131452号公報

【0007】

【特許文献2】

特開2002-251524号公報

【0008】

【非特許文献1】

A.Frier, P.Karlton, and P.Kocher, "The SSL 3.0 Protocol", [online], NetScape Communications Corp., Nov. 18, 1996, [平成15年1月17日検索], インターネット<URL: <http://wp.netscape.com/eng/ssl3/draft302.txt>>

【0009】

【発明が解決しようとする課題】

しかしながら、SACプロトコルや通信切断対策プロトコルは、その適用範囲を広げるために汎用性を重視し、それぞれ独立に提案されている。これにより、双方のプロトコルを利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となるという課題があった。

【0010】

より具体的には、SACプロトコルは端末装置とサーバ装置との間で最少でも2往復の通信が必要であり、通信切断対策プロトコルは最少でも1往復の通信が必要である。つまり、ライセンス配信プロトコルを開始する前に、3回の通信往復回数が必要となる。それゆえ、端末装置がライセンスを取得するまでに通信往復4回分の通信遅延が発生し、ユーザがコンテンツ利用要求を出してから、コンテンツの利用開始までに待ち時間が発生するという課題があった。

【0011】

本発明は、こうした従来の問題点を解決するものであり、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するととも

に、端末装置がライセンスを取得するまでの通信往復回数が2回であるプロトコルを実現するシステムおよび装置を提供することにより、ユーザがコンテンツの利用要求を出してから、コンテンツ利用開始までの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することを目的としている。

【0012】

【課題を解決するための手段】

上記目的を達成するために、本発明に関わるコンテンツ配信システムは、ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、前記サーバ装置および前記端末装置間の通信に、少なくとも前記サーバ装置による前記端末装置の正当性の認証と通信暗号鍵の共有を行う認証フェーズを含み、前記認証フェーズには、前記サーバ装置と前記端末装置間で通信されるトランザクションを識別する情報を交換するトランザクション識別情報交換フェーズと、前記トランザクションにおける前記端末装置からの先頭のコマンドを送信する先頭コマンド送信フェーズとを含むことにより、ユーザに対する応答時間を削減することを特徴とする。

【0013】

【発明の実施の形態】

（実施の形態1）

図1は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。図1において、本発明の一実施形態に係るコンテンツ配信システムは、サービス提供者側であるコンテンツ配信装置1と利用者側であるユーザ端末3とが、ネットワーク等の伝送路で接続される構成である。

【0014】

コンテンツ配信装置1は、コンテンツ購入処理部11と、ユーザ登録部12と、ユーザ権利登録部13と、ユーザ権利作成部14と、コンテンツ暗号化部15と、コンテンツ管理部16と、セキュリティ管理／通信部17と、ユーザデータベース18と、コンテンツ権利データベース19と、ユーザ所有権利データベー

ス20と、コンテンツデータベース21とを備えている。また、ユーザ端末3は、ユーザ指示処理部31と、端末情報記憶部32と、コンテンツ蓄積部33と、利用権利管理部34と、利用権利データベース35と、セキュリティ管理／通信部36と、出力部37とを備えている。

【0015】

まず、上記コンテンツ配信システムを構成するコンテンツ配信装置1およびユーザ端末3の概要を、以下に説明する。

コンテンツ配信装置1において、コンテンツ購入処理部11は、コンテンツ購入処理実行時に、コンテンツ権利データベース19に格納されている各コンテンツの内容、利用条件および料金等の情報を、ユーザ端末3へ送信してユーザに提示する。また、コンテンツ購入処理部11は、ユーザによってコンテンツが購入された場合には、ユーザ端末3からユーザ情報（ユーザID、端末ID、ユーザ名、電話番号等）を取得すると共に、必要な課金処理を行う。コンテンツ権利データベース19には、コンテンツ（映画やTV放送等の動画、書籍や印刷物等の静止画、ラジオ放送や朗読等の音声および音楽、ゲーム等）毎に、コンテンツ利用に関する1つ又は複数の情報が格納されている。

【0016】

ユーザ登録部12は、コンテンツ購入処理部11で取得されたユーザ情報を、ユーザデータベース18に記憶して登録する。ユーザデータベース18には、コンテンツ購入を行ったユーザの情報が、累積的に記憶されている。

【0017】

ユーザ権利登録部13は、ユーザ登録部12を介してコンテンツ購入処理部11から与えられる、ユーザが購入したコンテンツに関する情報を、ユーザが所有する権利としてユーザ所有権利データベース20に記憶して登録する。ユーザ所有権利データベース20には、ユーザが購入したコンテンツの利用権利が記憶されている。

【0018】

ユーザ権利作成部14は、ユーザ端末3から受けるコンテンツ利用要求に応じて、ユーザ端末3へ送信する利用権利（利用条件、コンテンツの復号鍵）を生成

する。

【0019】

コンテンツ暗号化部 15 は、ユーザ端末 3 へ送信するコンテンツの暗号化を行い、コンテンツデータベース 21 へ暗号化コンテンツの登録を行う。

コンテンツ管理部 16 は、ユーザ端末 3 へ送信する暗号化コンテンツをコンテンツデータベース 21 から検索し、セキュリティ管理／通信部 17 へ渡す。

【0020】

セキュリティ管理／通信部 17 は、ユーザ端末 3 の認証、コンテンツ配信装置 1 とユーザ端末 3 との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部 17 の構成および通信プロトコルの詳細については後述する。

【0021】

ユーザ端末 3 において、ユーザ指示処理部 31 は、ユーザが入力する指示（コンテンツ購入要求やコンテンツ利用要求等の指示）を処理する。

端末情報記憶部 32 には、上述したユーザ情報が記憶されている。

【0022】

コンテンツ蓄積部 33 には、購入によって取得された暗号化コンテンツが蓄積される。

利用権利管理部 34 は、コンテンツ利用要求に応答してコンテンツ配信装置 1 から送信されてくる利用権利を受信し、その内容に従って、対応するコンテンツの処理（暗号解読や利用条件に基づく再生等）を実行する。この利用権利は、利用権利データベース 35 に格納されて管理される。

【0023】

出力部 37 は、例えばディスプレイ等の表示装置であって、利用権利管理部 34 が実行する処理に応じてコンテンツの出力を行う。

セキュリティ管理／通信部 36 は、コンテンツ配信装置 1 の認証、コンテンツ配信装置 1 とユーザ端末 3 との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部 36 の構成および通信プロトコルの詳細については後述する。

【0024】

次に、コンテンツ配信装置1におけるセキュリティ管理／通信部17の構成の詳細について図2を用いて説明する。固有鍵情報記憶部201は、公開鍵暗号方式におけるコンテンツ配信装置1固有の公開鍵KD sが含まれるサーバ公開鍵証明書と、コンテンツ配信装置1固有の秘密鍵KE sと、認証局公開鍵証明書とを記憶する。サーバ公開鍵証明書はコンテンツ配信装置1の公開鍵KD sに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、一般的なX. 509証明書フォーマットを用いるものとする。公開鍵暗号方式およびX. 509証明書フォーマットについては、カーライル・アダムズ他著、鈴木優一訳、「PKIー公開鍵インフラストラクチャの概念、標準、展開」、ピアソンエデュケーション（2000/7）が詳しい。

【0025】

乱数発生部202は、乱数の生成を行う。生成された乱数は制御部204へ渡される。

暗号処理部203は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。データの暗号化および復号アルゴリズムにはAES（Advanced Encryption Standard）を、署名生成および署名検証アルゴリズムにはEC-D SA（Elliptic Curve Digital Signature Algorithm）を用いる。AESについてはNational Institute Standard and Technology（NIST）、FIPS Publication 197、EC-D SAについてはIEEE 1363 Standardが詳しい。

【0026】

暗号処理部203は、データの暗号化／復号を行う場合には、AES鍵と平文／暗号化データをそれぞれ入力とし、入力されたAES鍵で暗号化／復号したデータをそれぞれ出力する。また、署名生成／検証を行う場合には、署名対象データ／署名検証データと公開鍵／秘密鍵をそれぞれ入力とし、署名データ／検証結果をそれぞれ出力する。さらに、セッション鍵生成用パラメータの生成を行う場

合には、乱数を入力とし、Diffie-Hellmanパラメータを出力する。また、セッション鍵の生成を行う場合、乱数とDiffie-Hellmanパラメータを入力とし、セッション鍵を出力する。ここで、セッション鍵の生成にはECDH (Elliptic Curve Diffie-Hellman) を用いる。ECDHのアルゴリズムは、上記の IEEE 1363 Standardが詳しい。

【0027】

制御部204は、ユーザ端末3の認証処理、ユーザ端末3と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部204は、トランザクション毎にトランザクション識別子を割り当て、そのトランザクション識別子を通信ログデータベース206に保存することにより、通信切断対策処理を行う。ここで、トランザクションとは、「利用権利の取得」や「利用権利の返却」などの処理単位を表す。

【0028】

通信部205は、ユーザ端末3のセキュリティ管理／通信部36と通信を行う。

次に、ユーザ端末3におけるセキュリティ管理／通信部36の構成の詳細について図3を用いて説明する。固有鍵情報記憶部301は、公開鍵暗号方式におけるユーザ端末3固有の公開鍵KDcが含まれる端末公開鍵証明書と、ユーザ端末3固有の秘密鍵KEcと、認証局公開鍵証明書を記憶する。端末公開鍵証明書はユーザ端末3の公開鍵KDcに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、コンテンツ配信装置1と同様にX.509証明書フォーマットを用いる。

【0029】

乱数発生部302は、乱数の生成を行う。生成された乱数は制御部304へ渡される。

暗号処理部303は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。暗号処理部303の入出力は、コンテンツ配信装置1の暗号処理部203と同じである。

【0030】

制御部304は、コンテンツ配信装置1の認証処理、コンテンツ配信装置1と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部304は、コンテンツ配信装置1が生成したトランザクション識別子を通信ログデータベース306に蓄積することにより、通信切断対策処理を行う。

【0031】

通信部305は、ユーザ端末3側のセキュリティ管理／通信部17と通信を行う。

次に、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ配信方法を、図4～図12を参照して具体的に説明する。

【0032】

図4は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入に関する処理を説明するフローチャートである。図5は、コンテンツ権利データベース19に格納されているコンテンツに関する情報の一例を概念的に示す図である。図6は、ユーザデータベース18に格納されているユーザ情報の一例を概念的に示す図である。図7は、ユーザ所有権利データベース20に格納されているユーザが所有する権利の情報の一例を概念的に示す図である。図8は、コンテンツデータベース21に格納されているコンテンツ情報の一例を概念的に示す図である。図9は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。図10～図12は、本発明の一実施形態に係るコンテンツ配信システムで行われる秘匿通信と通信切断対策処理を説明するフローチャートである。

【0033】

(1) コンテンツ購入処理

図4を参照して、コンテンツ配信装置1で提供されるコンテンツをユーザが購入する際に、コンテンツ配信システムで行われる処理を説明する。

【0034】

ユーザ端末3では、ユーザが、コンテンツ購入に関する指示をユーザ指示処理部31へ出力する。ユーザ指示処理部31は、セキュリティ管理／通信部36を

介して、指示に応じたコンテンツ購入要求をコンテンツ配信装置 1 へ発行する（ステップ S 4 1）。

【0035】

コンテンツ配信装置 1 では、ユーザ端末 3 から発行されたコンテンツ購入要求が、セキュリティ管理／通信部 1 7 を介してコンテンツ購入処理部 1 1 で受信される。コンテンツ購入処理部 1 1 は、コンテンツ購入要求を受信すると、コンテンツ権利データベース 1 9 から格納されているすべてのコンテンツに関する情報を取得し、セキュリティ管理／通信部 1 7 を介してユーザ端末 3 へ送信する（ステップ S 4 2）。

【0036】

ここで、コンテンツ権利データベース 1 9 には、例えば図 5 に示すような情報が格納されている。図 5 において、コンテンツ名は、コンテンツの名称であり、コンテンツ ID は、コンテンツを識別するために付される固有の番号である。利用条件は、通常使用される予め定めたデータ形式によって、コンテンツを利用できる具体的な条件を示すものである。各コンテンツに設定される利用条件および金額は、1 つであってもよいし、複数であってもよい。この例では、映画 A というコンテンツには、再生回数による利用条件が設定されており、400 円を支払えば、映画 A を 2 回観賞することができることを表している。

【0037】

なお、利用条件には、上述した利用回数や利用時間以外にも、利用期間、記録媒体へのコピーや書面への印刷の可否等の様々な条件を使用することが可能である。

【0038】

再び図 4 を参照して、ユーザ端末 3 において、コンテンツ購入処理部 1 1 から送信されたコンテンツに関する情報（図 5）が確認され、ユーザがいずれかのコンテンツの購入を決定した場合（ステップ S 4 3, Yes）、ユーザ指示処理部 3 1 は、コンテンツ購入決定通知（購入したコンテンツおよび選択した利用条件の情報を含む）と共に、端末情報記憶部 3 2 に格納されているユーザ情報を、セキュリティ管理／通信部 3 6 を介してコンテンツ配信装置 1 へ送信する（ステッ

プ S 4 4)。

【0039】

コンテンツ配信装置 1 では、ユーザ端末 3 から送信されるコンテンツ購入決定通知およびユーザ情報を、セキュリティ管理／通信部 1 7 を介してコンテンツ購入処理部 1 1 で受信する。そして、コンテンツ購入処理部 1 1 は、必要な課金処理を実行すると共に、購入されたコンテンツの情報とユーザ情報とを、ユーザ登録部 1 2 へ送出する (ステップ S 4 5)。なお、課金処理は本発明の主眼ではないので、説明を省略する。

【0040】

ユーザ登録部 1 2 は、コンテンツ購入処理部 1 1 から送出される購入されたコンテンツの情報およびユーザ情報を、ユーザ権利登録部 1 3 へ転送すると共に、ユーザ情報をユーザデータベース 1 8 に記憶して登録する (ステップ S 4 7)。このとき、コンテンツ購入処理部 1 1 から送出されるユーザ情報と同一の内容が、既にユーザデータベース 1 8 に登録されている場合には、上述したユーザ登録は行われぬ (ステップ S 4 6, Yes)。

【0041】

ユーザデータベース 1 8 には、例えば図 6 に示すような情報が格納される。図 6 において、ユーザ ID は、ユーザを識別するために付される固有の番号である。ユーザ名は、ユーザの名前である。端末 ID は、端末を識別するために付される固有の番号であり、1 人のユーザが複数の端末を所有している場合等に利用される。電話番号は、ユーザを特定するために利用される。図 6 の例では、“ID 番号「0001」である「一朗」というユーザが、ID 番号「1234567」の端末を利用する”という内容が、ユーザ情報として登録されている。

【0042】

ユーザ権利登録部 1 3 は、購入によってユーザが所有することになるコンテンツ利用の権利を、ユーザ登録部 1 2 から与えられる購入されたコンテンツの情報とユーザ情報とに基づいて、ユーザ所有権利データベース 2 0 に記憶して登録する (ステップ S 4 8)。

【0043】

ユーザ所有権利データベース 20 には、例えば図 7 に示すような情報が格納されている。図 7 において、ユーザ ID は、ユーザデータベース 18 に登録されている情報である。コンテンツ ID および利用条件は、コンテンツ権利データベース 19 に登録されている情報である。

【0044】

上記処理によって、コンテンツの購入およびその購入に伴うユーザの所有権利の登録が完了する。

(2) コンテンツ利用処理

次に、図 9 を参照して、上述した処理によってユーザ所有権利データベース 20 にユーザ所有権利が登録された後、ユーザが購入したコンテンツを利用する際にコンテンツ配信システムで行われる処理を説明する。

【0045】

ユーザ端末 3 では、ユーザが、コンテンツ利用に関する指示をユーザ指示処理部 31 へ出力する。このとき、ユーザは、コンテンツをどのように利用するのかの指示を与える。例えば、購入したコンテンツの利用条件が回数であれば何回利用したいのか、時間であれば何分利用したいのかという指示を与える。ユーザ指示処理部 31 は、セキュリティ管理／通信部 36 を介して、指示に応じたコンテンツ利用要求をコンテンツ配信装置 1 へ送信する（ステップ S91）。なお、コンテンツ利用要求は、必ずしもユーザ指示に従って作成されるものではなく、ユーザ端末 3 内で自動的に作成される場合もある。例えば、端末 3 がサポートするコンテンツの利用条件が固定されている場合、ユーザが指示を与えるまでもなく、コンテンツ利用要求をユーザ端末 3 内で作成することができる。具体的には、ユーザ端末 3 が、記憶容量の制限により毎回 1 回分の利用権利だけが取得・処理可能な端末の場合であり、この場合には端末に応じたコンテンツ利用要求をユーザ指示処理部 31 で自動的に作成し、コンテンツ配信装置 1 へ発行する。このコンテンツ利用要求には、上記指示の内容、ユーザ ID、端末 ID およびコンテンツ ID が含まれる。

【0046】

コンテンツ配信装置 1 では、ユーザ端末 3 から送信されたコンテンツ利用要求

を、セキュリティ管理／通信部 17 を介してユーザ権利作成部 14 で受信する。ユーザ権利作成部 14 は、コンテンツ利用要求を受信すると、この要求に対応した内容が登録されているか否かを、ユーザデータベース 18 およびユーザ所有権利データベース 20 を参照して確認する（ステップ S 9 2）。具体的には、ユーザ権利作成部 14 は、コンテンツ利用要求に含まれるユーザ ID および端末 ID が、ユーザデータベース 18 に登録されているか否かをまず確認し、登録されていると判断すると、そのユーザ ID においてコンテンツ利用要求に含まれるコンテンツ ID および指示に応じた利用条件が、ユーザ所有権利データベース 20 に登録されているか否かを確認する。

【0047】

上記ステップ S 9 2 における確認の結果、コンテンツ利用要求に対応した内容が登録されていると判断した場合（ステップ S 9 3, Yes）、ユーザ権利作成部 14 は、コンテンツ利用要求に応じた利用権利を作成し、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ送信する（ステップ S 9 4）。また、ユーザ権利作成部 14 は、コンテンツ利用要求に含まれるコンテンツ ID をコンテンツ管理部 16 へ通知する。コンテンツ管理部 16 は、コンテンツ ID に対応するコンテンツをコンテンツデータベース 21 から取り出し、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ送信する（ステップ S 9 5）。

【0048】

一方、上記ステップ S 9 2 における確認の結果、コンテンツ利用要求に対応した内容が登録されていないと判断した場合（ステップ S 9 3, No）、ユーザ権利作成部 14 は、コンテンツ利用要求を拒絶する旨を、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ通知する（ステップ S 9 7）。

【0049】

ここで、上記ステップ S 9 4 で行われる利用権利の生成は、次のようにして行われる。前提として、ユーザ ID 「0001」のユーザが、図 7 のユーザ所有権利データベース 20 に示される登録内容で、事前にコンテンツの購入を行っていたと仮定する。

【0050】

さらに、そのユーザが、コンテンツID「112233」のコンテンツを1回利用したいというコンテンツ利用要求を送信してきた場合を考える。この場合、ユーザ所有権利データベース20に登録されている利用条件が2回であるので、ユーザ権利作成部14は、要求通り再生回数=1を与える情報および該当コンテンツの復号鍵を含む利用権利を作成する。また、ユーザ権利作成部14は、この利用権利の作成と同時に、ユーザ所有権利データベース20に登録されている利用条件の回数を1つ減少させて、登録内容を更新する（図7の例では、2→1）。ただし、通信切断対策処理において、セキュリティ管理／通信部17から再開トランザクションとして指示された場合には、登録内容の更新を行わない。なお、通信切断対策処理については後述する。

【0051】

なお、ユーザ権利作成部14は、通信切断対策処理により再開トランザクションが発行されることを想定して、作成したユーザ権利を保存しておいてもよい。これにより、再開トランザクション発行時にユーザ権利を再度作成する手間を省くことができる。

【0052】

なお、ユーザ端末3へ利用権利を発行する毎に、ユーザ所有権利データベース20に登録されている内容を更新した結果、コンテンツの購入によって与えられた利用条件がなくなった場合には、ユーザ所有権利データベース20に登録されている該当ユーザ所有権利を削除してもよいし、そのまま残しておいてもよい。残しておく場合には、同一のユーザが再度同じコンテンツの購入を行ったときや、ユーザが取得した利用権利を行使せずに返却するとき等に、処理対応がしやすくなる。

【0053】

再び図9を参照して、ユーザ端末3において、コンテンツ配信装置1から送信される暗号化コンテンツは、コンテンツ蓄積部33に蓄積され、利用権利は、利用権利管理部34に入力される。利用権利管理部34は、取得した利用権利に含まれる復号鍵を用いて該当コンテンツに施された暗号を解読し、利用条件に従って暗号解読したコンテンツの再生処理等を、出力部37を通して実行する（ステ

ップS96)。なお、取得された利用権利は、利用権利データベース35に格納され、コンテンツの再生回数や累積時間等の管理に利用される。

【0054】

上記処理によって、要求される利用条件に応じたコンテンツを配信することができる。

(3) 秘匿通信・通信切断処理

次に、図10～図12を参照して、上述したコンテンツ利用処理において、利用権利の要求(図9のステップS91)、および、利用権利の配信(図9のステップS95)の際に、セキュリティ管理／通信部17、36で行われる、ユーザ端末3の認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理を説明する。

【0055】

図10は、コンテンツ利用処理におけるユーザ端末3とコンテンツ配信装置1との1回目の通信往復で行われる処理について記述している。また、図11は、前記1回目の通信往復後、2回目の通信往復を開始する前にユーザ端末3において行われる処理について記述している。さらに、図12はコンテンツ利用処理におけるユーザ端末3とコンテンツ配信装置1との2回目の通信往復で行われる処理について記述している。

【0056】

ユーザ端末3のセキュリティ管理／通信部36に含まれる制御部304は、ユーザ指示処理部31からコンテンツ利用要求の送信を指示された場合、乱数発生部302で生成した乱数Rcと、固有情報記憶部301に記憶している端末公開鍵証明書と、コンテンツ利用要求とを、通信部305を介して、コンテンツ配信装置1へ送信する(ステップS1001)。

【0057】

コンテンツ配信装置1のセキュリティ管理／通信部17に含まれる制御部204は、通信部205を介してユーザ端末3から、乱数Rc、端末公開鍵証明書、コンテンツ利用要求を受信すると、まず、固有情報記憶部201に記憶している認証局公開鍵証明書と、前記端末公開鍵証明書とを、暗号処理部203に与える

ことにより、前記端末公開鍵証明書の署名検証を行う（ステップS1002）。

【0058】

上記ステップS1002における署名検証の結果、検証失敗となった場合（ステップS1003, No）、制御部204は、コンテンツ利用要求を拒絶する旨を、通信部205を介してユーザ端末3へ通知する（ステップS1004）。

【0059】

一方、上記ステップS1002における署名検証の結果、検証が成功した場合（ステップS1003, Yes）、制御部204は、乱数生成部202で乱数Rs、TID、およびRs2を生成し、暗号処理部203で、乱数Rs2を入力としてDiffie-HellmanパラメータDHsの生成を行う（ステップS1005）。ここでTIDは、このコンテンツ要求トランザクションに対応付けられた識別子であり、今後、通信切断が発生した場合には、このトランザクション識別子TIDを用いて、中断されたトランザクションの再開が行われる。

【0060】

さらに、制御部204は、ユーザ端末3から受信した乱数Rc、ステップS1005で生成したTID、ステップS1005で生成したDHsを連結したデータ（式1）の署名（式2）を暗号処理部203で生成する（ステップS1006）。

$$Rc || TID || DHs \quad (\text{式1})$$

$$S(s, Rc || TID || DHs) \quad (\text{式2})$$

【0061】

制御部204は、ステップS1005で生成した乱数Rs、トランザクション識別子TID、Diffie-HellmanパラメータDHsと、固有鍵情報記憶部201に記憶しているサーバ公開鍵証明書と、ステップS1006で生成した署名（式2）をユーザ端末3に通信部205を介して送信する（ステップS1007）。

【0062】

ユーザ端末3のセキュリティ管理／通信部36に含まれる制御部304は、通信部305を介してコンテンツ配信装置1から、乱数Rs、トランザクション識

別子TID、Diffie-HellmanパラメータDH_s、サーバ公開鍵証明書、および署名データを受信すると、まず、固有情報記憶部301に記憶している認証局公開鍵証明書と、前記サーバ公開鍵証明書とを、暗号処理部303に与えることにより、前記サーバ公開鍵証明書の署名検証を行う（ステップS1101）。

【0063】

上記ステップS1101における署名検証の結果、検証失敗となった場合（ステップS1102, No）、制御部304は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部31へ通知する（ステップS1103）。

【0064】

一方、上記ステップS1101における署名検証の結果、検証が成功した場合（ステップS1102, Yes）、制御部304は、ステップS1001で作成した乱数R_cとステップS1007でコンテンツ配信装置1から受信したTID、およびDH_sを結合したデータ（式3）を生成し、そのデータ（式3）、ステップS1007でコンテンツ配信装置1から受信した署名データ（式2）、およびサーバ公開鍵証明書を暗号処理部303に入力し、署名データ（式2）の検証を行う（ステップS1104）。

$$R_c || TID || DH_s \quad (式3)$$

【0065】

上記ステップS1104における署名検証の結果、検証失敗となった場合（ステップS1105, No）、制御部304は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部31へ通知する（ステップS1103）。

【0066】

一方、上記ステップS1104における署名検証の結果、検証が成功した場合（ステップS1105, Yes）、ユーザ端末3は通信相手が確かにコンテンツ配信装置1であることがわかる（通信相手の認証）。制御部304は、乱数発生部302で生成した乱数R_{c2}を暗号処理部303の入力としてDiffie-HellmanパラメータDH_cを生成する（ステップS1106）。

【0067】

さらに、制御部304は、ステップS1007でコンテンツ配信装置1から受信したDHsと、ステップS1106で生成したRc2とから、暗号処理部303でセッション鍵KSを生成する（ステップS1107）。

【0068】

その後、制御部304は、ステップS1007でコンテンツ配信装置1から受信したTIDとRs、ステップS1106で生成したDHcとKSを通信ログデータベース306に記憶する（ステップS1108）。これにより、TIDに対応するコンテンツ利用権利要求トランザクションが、このステップまで完了したことがデータベースに保存される。よって、これ以降、通信切断などによりトランザクションが中断された場合には、この次のステップから処理を再開すればよいこととなる。

【0069】

制御部304は、コンテンツ配信端末1から受信した乱数RsとTID、ステップS1106で生成したDHcを連結したデータ（式4）の署名（式5）を暗号処理部303で生成する（ステップS1109）。

$$Rs || TID || DHc \quad (式4)$$

$$S(c, Rs || TID || DHc) \quad (式5)$$

【0070】

制御部304は、TIDと、ステップS1106で生成したDHcと、ステップS1109で生成した署名（式5）をコンテンツ配信装置1に通信部305を介して送信する（ステップS1110）。

【0071】

コンテンツ配信装置1のセキュリティ管理／通信部17に含まれる制御部204は、通信部205を介してユーザ端末3から、トランザクション識別子TID、Diffie-HellmanパラメータDHc、および署名データを受信すると、ステップS1005で作成した乱数RsとステップS1110でユーザ端末3から受信したTID、およびDHcを結合したデータ（式6）を生成し、そのデータ（式6）、ステップS1110でユーザ端末3から受信した署名データ、および端末公開鍵証明書を暗号処理部203に入力し、署名データの検証を行

う (ステップ S1201)。

$$Rs || TID || DHc \quad (式6)$$

【0072】

上記ステップ S1201 における署名検証の結果、検証失敗となった場合 (ステップ S1202, No)、制御部 204 は、コンテンツ利用要求を拒絶する旨を、通信部 205 を介してユーザ端末 3 へ通知する (ステップ S1203)。

【0073】

一方、上記ステップ S1201 における署名検証の結果、検証が成功した場合 (ステップ S1202, Yes)、コンテンツ配信装置 1 は通信相手が確かにユーザ端末 3 であることがわかる (通信相手の認証)。制御部 204 は、ステップ S1201 でユーザ端末 3 から受信した DHc と、ステップ S1005 で生成した Rs2 とから、暗号処理部 203 でセッション鍵 KS を生成する (ステップ S1204)。

【0074】

さらに、制御部 204 は、通信ログデータベースを検索し、ステップ S1201 でユーザ端末 3 から受信した TID が存在するかを調べる。その結果、TID が既に存在しない場合 (ステップ S1205, No)、制御部 204 は、ステップ S1201 でユーザ端末 3 から受信した TID と、ステップ S1204 で生成した KS を通信ログデータベース 206 に記憶する (ステップ S1206)。これにより、TID に対応するコンテンツ利用権利要求トランザクションが、このステップまで完了したことがデータベースに保存される。よって、これ以降、通信切断などによりトランザクションが中断された場合には、この次のステップから処理を再開すればよいこととなる。

【0075】

その後、制御部 204 はユーザ権利生成部 14 に新規トランザクションとして、ステップ S1001 でユーザ端末 3 から受信したコンテンツ利用要求を通知する (ステップ S1207)。

【0076】

一方、TID が既に存在する場合 (ステップ S1205, Yes)、制御部 2

04 は、ユーザ権利生成部 14 に再開トランザクションとして、ステップ S1001 でユーザ端末 3 から受信したコンテンツ利用要求を通知する（ステップ S1208）。

【0077】

制御部 204 は、TID とユーザ権利作成部 14 で作成された利用権利を結合し、さらに、ステップ S1204 で生成したセッション鍵 KS を用いて暗号処理部 203 で暗号化して、通信部 205 を介してユーザ端末 3 に送信する（ステップ S1209）。ここで、送信される利用権利は、コンテンツ配信端末 1 とユーザ端末 3 のみで生成可能なセッション鍵 KS で暗号化されているため、第三者が盗聴することはできない。

【0078】

最後に、ユーザ端末 3 のセキュリティ管理／通信部 36 に含まれる制御部 304 は、通信部 305 を介してコンテンツ配信装置 1 から、暗号化データを受信すると、まず、暗号処理部 303 でセッション鍵 KS を用いて暗号化データの復号を行い、TID と利用権利を復元する。さらに、通信ログデータベース 306 から、暗号化データに含まれる TID に対応するデータを削除する。（ステップ S1210）。

【0079】

上記処理により、ユーザ端末の認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理を行うことが可能となる。

なお、上記処理の完了後、ユーザ端末 3 は、コンテンツ配信装置 1 の通信ログデータベース 206 に保存されている不要な情報を削除するため、トランザクション完了通知をコンテンツ配信装置 1 に送信してもよい。トランザクション完了通知は完了したトランザクションの TID をセッション鍵 KS で暗号化したものである。トランザクション完了通知を受信したコンテンツ配信装置 1 は、TID に対応するデータを通信ログデータベース 206 から削除する。

【0080】

なお、本実施の形態で用いた暗号アルゴリズム、セッション鍵共有アルゴリズム、証明書フォーマットなどは、同等の機能を持つものであれば、必ずしも記載

したものを用いる必要はない。例えば、データの暗号アルゴリズムにはT r i p l e D E Sを用いてもよい。また、公開鍵暗号方式の代わりに共通鍵暗号方式を用いてもよい。

【0081】

なお、本実施の形態では、ユーザ端末3からのコンテンツ利用要求と端末公開鍵証明書は、1往復目の通信（図10のステップS1001）において送信したが、2往復目の通信（図11のステップS1110）において送信してもよい。これにより、コンテンツ配信装置1は、装置内に上記データを保持しておく必要がなくなる。この場合、コンテンツ配信装置1での端末公開鍵証明書の署名検証処理（図10のステップS1102）は、2往復目の最初（図12のステップS1201の直前）で行うこととなる。

【0082】

なお、ステップS1007において、コンテンツ配信装置1からユーザ端末3へ送信されるデータに、ユーザ端末3から受信した乱数R_cを含めてもよい。つまり、コンテンツ配信装置1から送信されるデータは、乱数R_c、乱数R_s、TID、パラメータDH_s、署名データとなる。これにより、ユーザ端末3は、乱数R_cを端末内に保持しておく必要がなくなる。同様に、ステップS1110において、ユーザ端末3からコンテンツ配信装置1へ送信されるデータに、コンテンツ配信装置1から受信した乱数R_sを含めてもよい。つまり、コンテンツ配信装置1から送信されるデータは、乱数R_s、TID、パラメータDH_c、署名データとなる。

【0083】

なお、本実施の形態において、TIDはコンテンツ配信装置1が生成したが、ユーザ端末3で生成してもよい。この場合、ステップS1001において、ユーザ端末3はコンテンツ配信装置1に対して、生成したTIDを送信する。

【0084】

なお、本実施の形態においては、ユーザ端末3がコンテンツ配信装置1を認証する処理も含まれているが、特に必要がない場合には、認証処理を除いてもよい。

【0085】

なお、本実施の形態においては、ステップS94においてユーザ権利の作成を行う際に、セキュリティ管理／通信部17から再開トランザクションとして指示された場合には、登録内容の更新を行わないとしたが、再度、コンテンツ利用要求を評価し、ユーザ権利の作成をやり直してもよい。これにより、新規トランザクションの発行と再開トランザクションの発行の間に起こった状況変化に対応することが可能となる。例を挙げれば、新規トランザクション発行時には、コンテンツの利用有効期限内であったので利用権利の作成・送信を行なったが、再開トランザクションとして再度要求が行われたときには、コンテンツの利用有効期限を越えたいた場合が考えられる。この場合には、再開トランザクションに対しては利用権利の作成・発行は行わない。

【0086】

なお、本実施の形態では、1つのトランザクション処理についての例を示したが、複数のトランザクション処理を行う場合には、例示した処理を複数回行えばよい。複数トランザクション処理において、さらに、応答時間を削減したい場合には、2回目以降の認証処理を除いてもよい。つまり、認証処理は最初の1度だけ行い、同じセッション鍵KSを再利用する。さらに、複数のトランザクションを逐次的に実行するのではなく、並列的に実行してもよい。これにより、1トランザクションあたりの応答時間が削減される。

【0087】

また、コンテンツ配信装置1とユーザ端末3との間の2つのコンテンツ利用要求処理を処理Aおよび処理Bとすると、処理Aの終了後に、一旦、通信切断を行わなければいけない場合、通常は、処理Bの開始時には再度認証処理を行い、新たなセッション鍵を作成しなおすが、処理Bの応答時間を削減したい場合には、処理Bでの認証処理を除くために、処理Aでのセッション鍵をコンテンツ配信装置1とユーザ端末3の双方で記憶しておき、再利用してもよい。

【0088】

なお、上記のように、セッション鍵の再利用を行う際、コンテンツ配信装置1はセッション鍵の利用制限を設けてもよい。例えば、セッション鍵の再利用回数

が規定の上限を超えた場合、セッション鍵が最初に作成されたから規定の時間が経過した場合、セッション鍵が最初に作成されてから規定の通信データ量を超えた場合、予め決められたコンテンツあるいは利用権利を配信する場合、あるいは、予め決められたユーザ端末3に配信する場合などに、コンテンツ配信装置1はユーザ端末3にセッション鍵再利用不可通知を行う。セッション鍵再利用不可通知を受信したユーザ端末3は、セッション鍵を生成しなおす。つまり、ステップ1001から通信をやり直す。

【0089】

なお、本実施の形態で示したコンテンツ配信システムの各構成要素は、ハードウェアで実現しても、ソフトウェアで実現してもよい。

【0090】

【発明の効果】

以上のように本発明によれば、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、端末装置がライセンスを取得するまでの通信往復回数が2回であるプロトコルを実現するシステムおよび装置を提供することにより、ユーザがコンテンツの利用要求を出してから、コンテンツ利用開始までの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することができる。

【図面の簡単な説明】

【図1】

本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図

【図2】

本発明の一実施形態に係るコンテンツ配信システムの構成のコンテンツ配信装置のセキュリティ管理／通信部を示すブロック図

【図3】

本発明の一実施形態に係るコンテンツ配信システムの構成のユーザ端末のセキュリティ管理／通信部を示すブロック図

【図4】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入

に関する処理を説明するフローチャート

【図 5】

コンテンツ権利データベース 19 に格納されているコンテンツに関する情報の一例を概念的に示す図

【図 6】

ユーザデータベース 18 に格納されているユーザ情報の一例を概念的に示す図

【図 7】

ユーザ所有権利データベース 20 に格納されているユーザが所有する権利の情報の一例を概念的に示す図

【図 8】

コンテンツデータベース 21 に格納されているコンテンツ情報の一例を概念的に示す図

【図 9】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャート

【図 10】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との 1 回目の通信往復で行われる処理を説明するフローチャート

【図 11】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との 1 回目の通信往復後、2 回目の通信往復を開始する前にユーザ端末 3 において行われる処理を説明するフローチャート

【図 12】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との 2 回目の通信往復で行われる処理を説明するフローチャート

【符号の説明】

- 1 コンテンツ配信装置
- 3 ユーザ端末
- 1 1 コンテンツ購入処理部
- 1 2 ユーザ登録部
- 1 3 ユーザ権利登録部
- 1 4 ユーザ権利作成部
- 1 5 コンテンツ暗号化部
- 1 6 コンテンツ管理部
- 1 7, 3 6 セキュリティ管理／通信部
- 1 8 ユーザデータベース
- 1 9 コンテンツ権利データベース
- 2 0 ユーザ所有権利データベース
- 2 1 コンテンツデータベース
- 3 1 ユーザ指示処理部
- 3 2 端末情報記憶部
- 3 3 コンテンツ蓄積部
- 3 4 利用権利管理部
- 3 5 利用権利データベース
- 3 7 出力部
- 2 0 1 固有鍵情報記憶部
- 2 0 2 乱数発生部
- 2 0 3 暗号処理部
- 2 0 4 制御部
- 2 0 5 通信部
- 2 0 6 通信ログデータベース
- 3 0 1 固有鍵情報記憶部
- 3 0 2 乱数発生部
- 3 0 3 暗号処理部
- 3 0 4 制御部

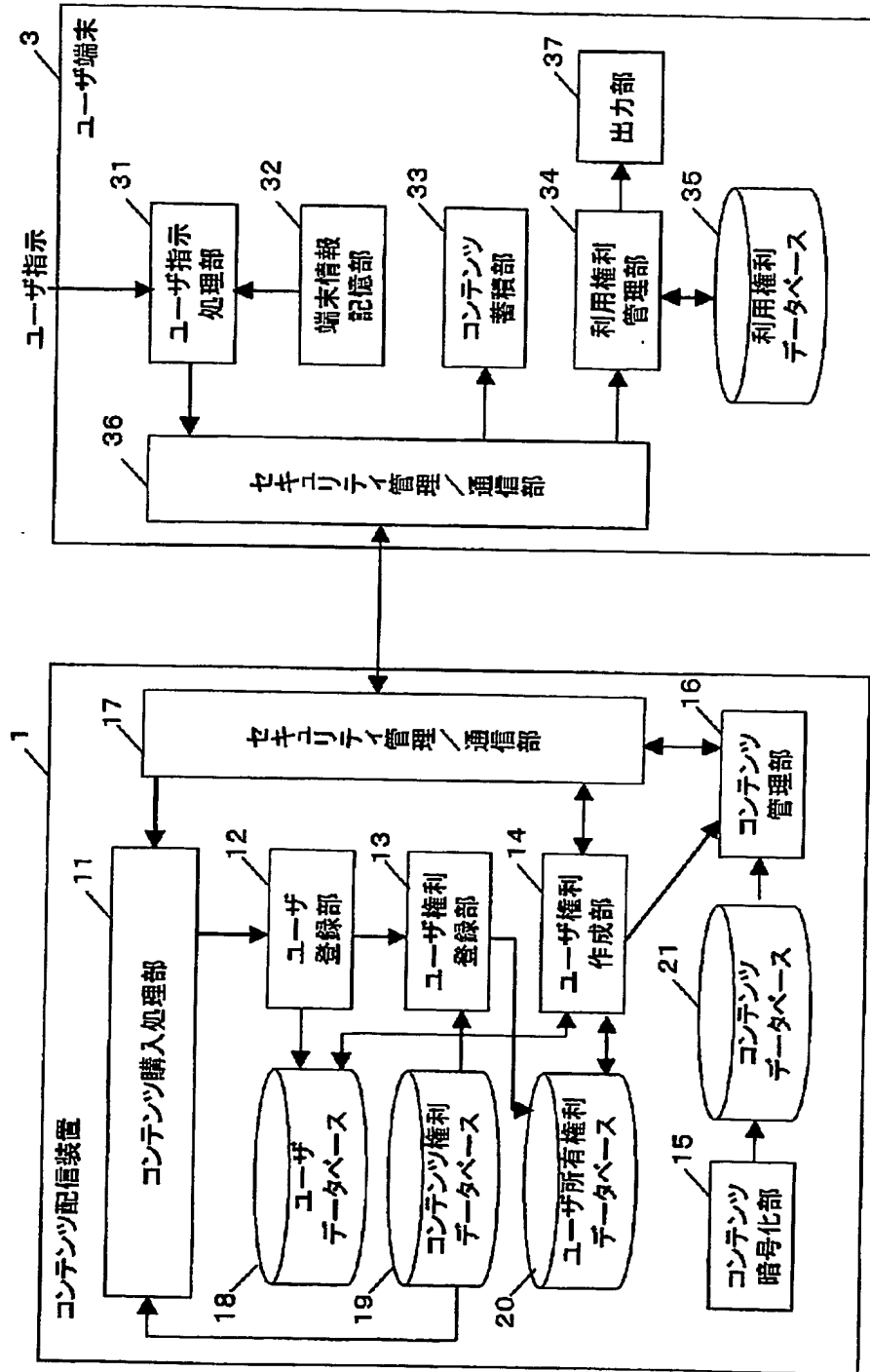
3 0 5 通信部

3 0 6 通信ログデータベース

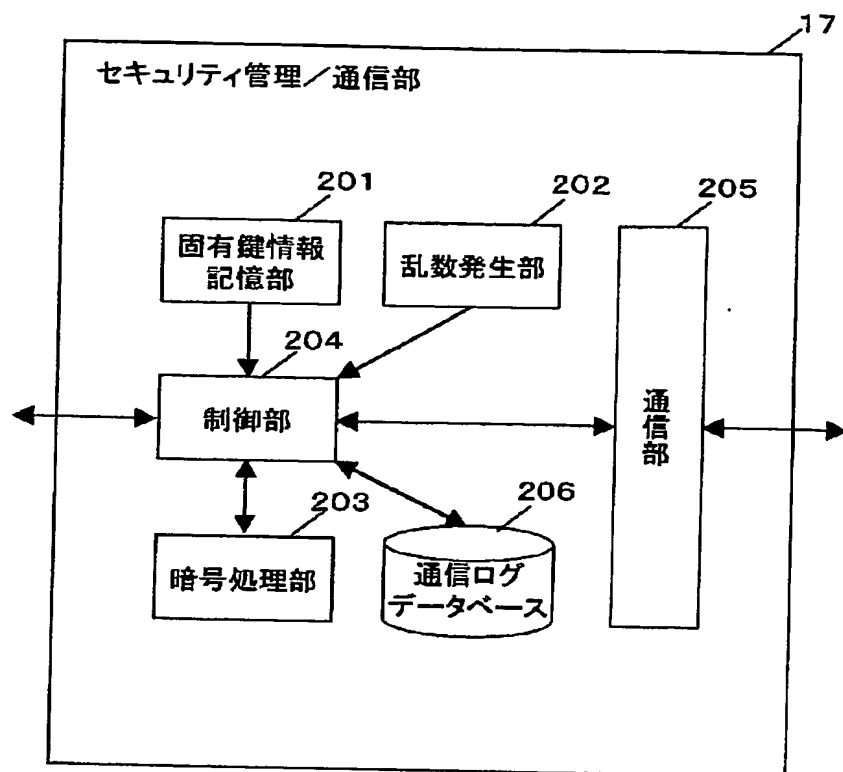
【書類名】

図面

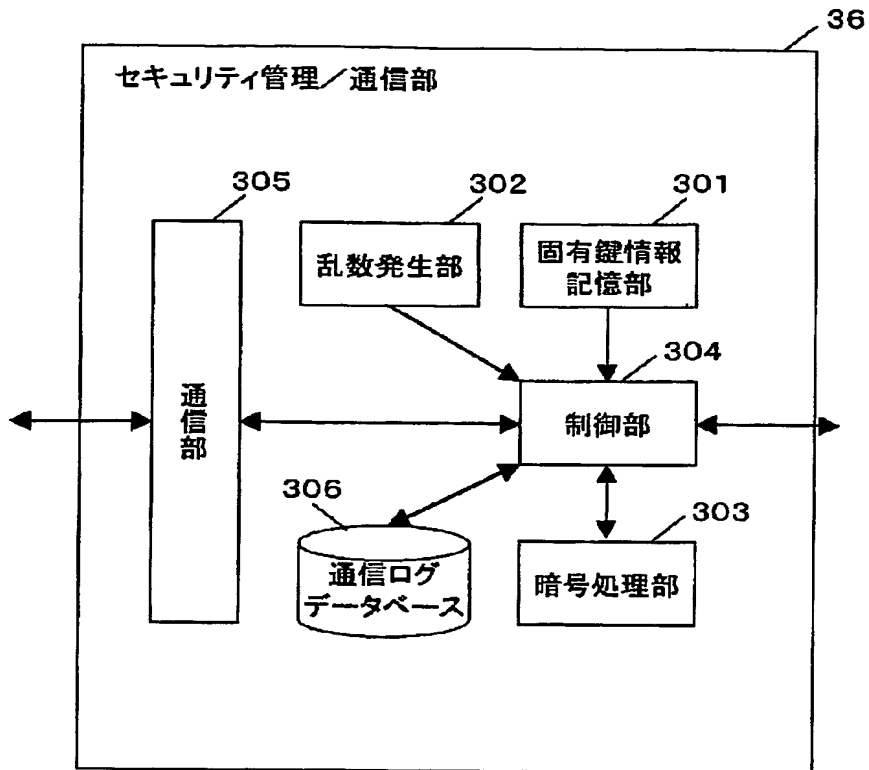
【図 1】



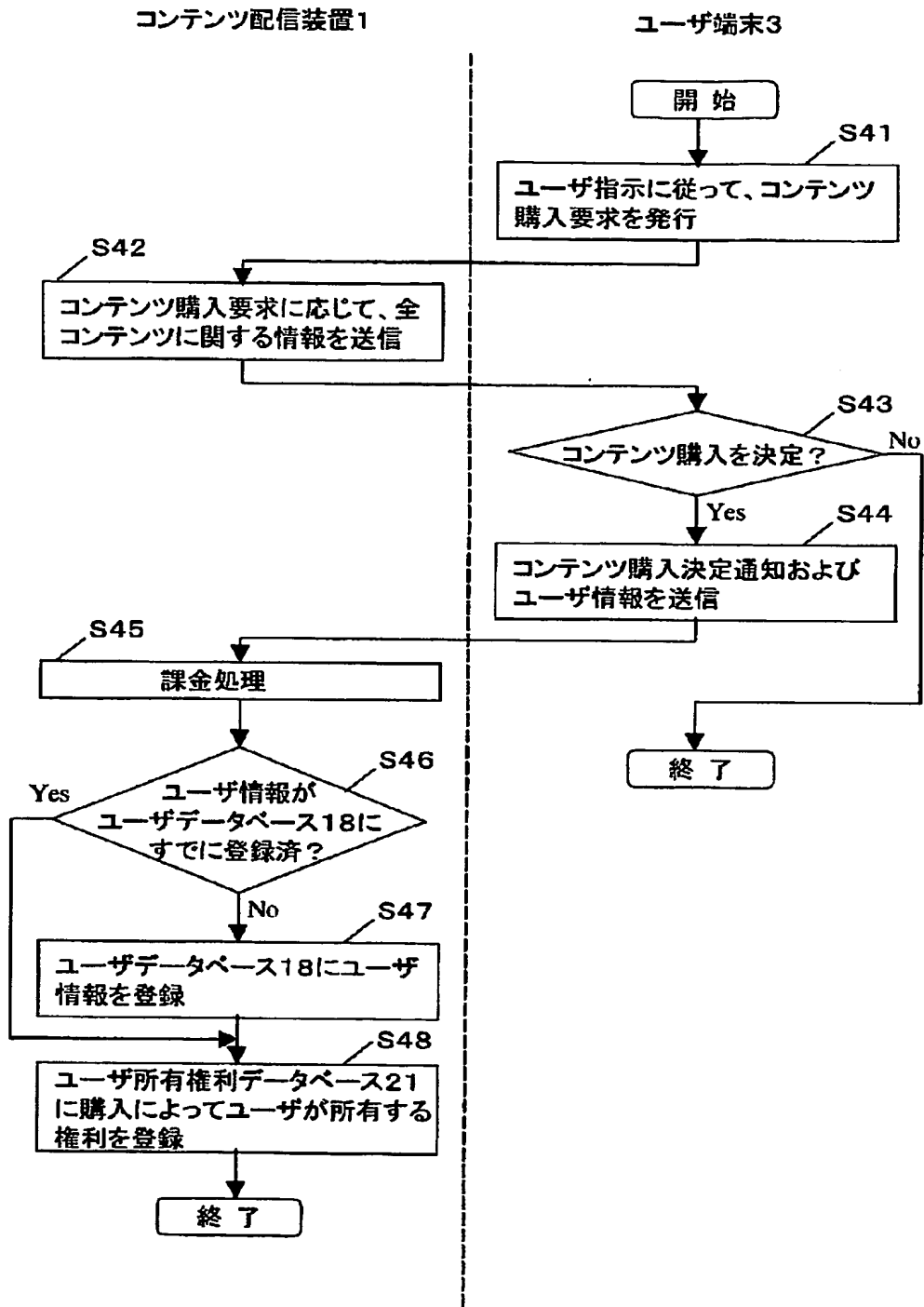
【図 2】



【図 3】



【図 4】



【図 5】

コンテンツ名	コンテンツID	利用条件	料金
映画A	112233	再生回数=2	400円
音楽B	334567	再生回数=5 累積再生時間=1H	500円 1000円
ゲームC	321098	累積再生時間=2H 無制限	700円 2000円

【図 6】

ユーザID	ユーザ名	端末ID	電話番号
0001	一朗	1234567	06-XXXX-XXXX
0002	太郎	1170930	03-YYYY-YYYY

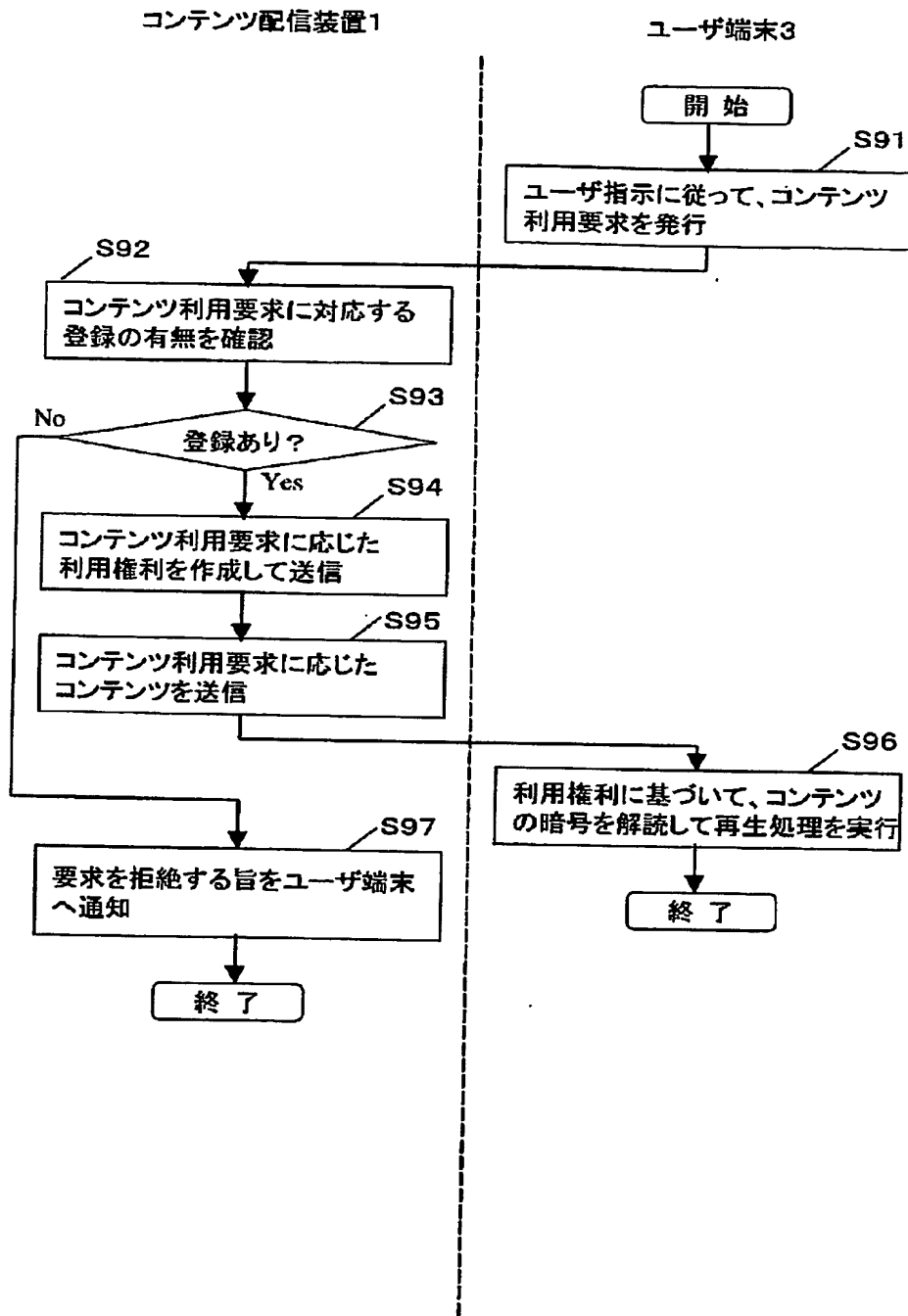
【図 7】

ユーザID	コンテンツID	利用条件
0001	112233	再生回数=2
0002	321098	累積再生時間=2H

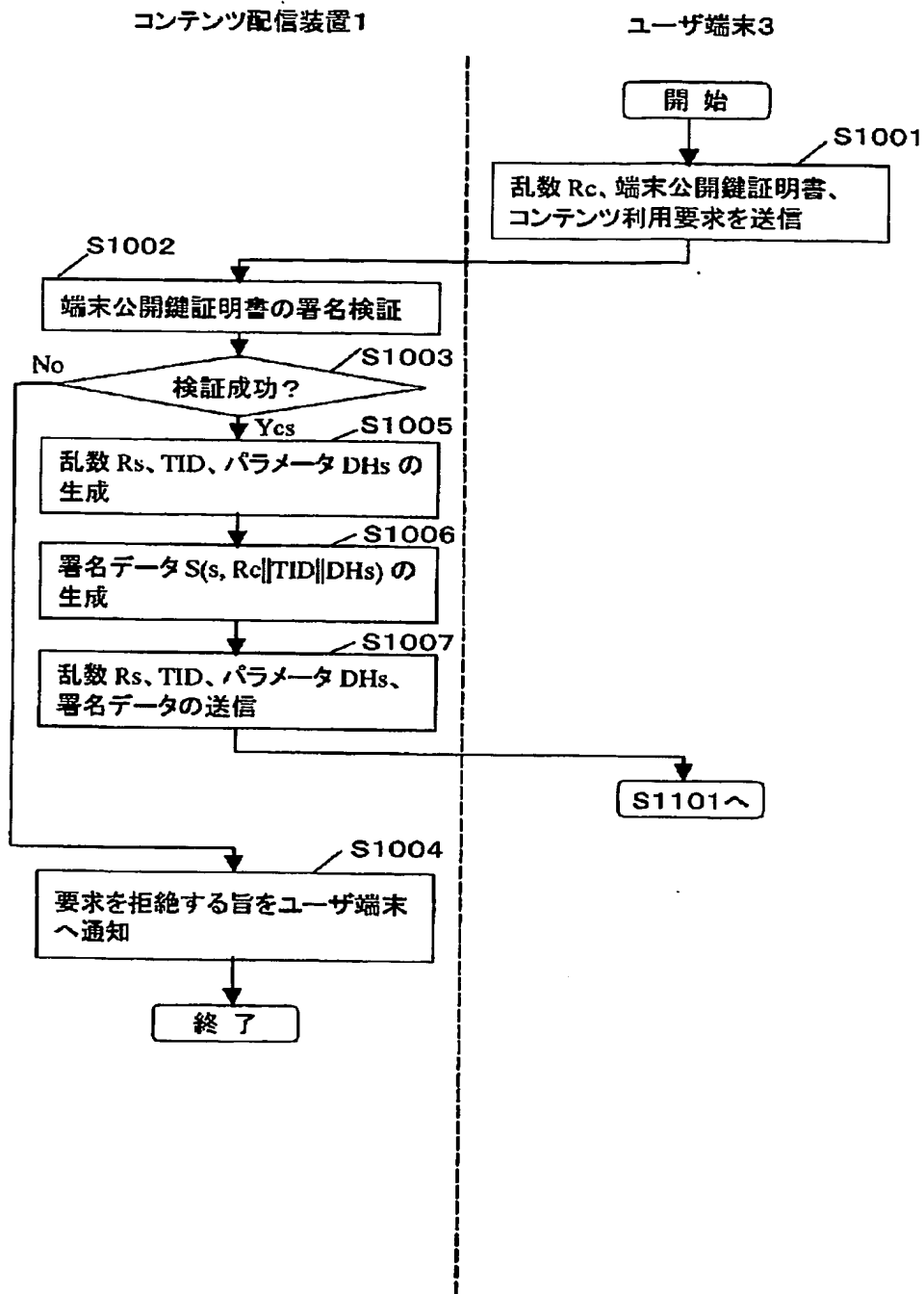
【図 8】

コンテンツID	コンテンツ名	コンテンツ暗号鍵	ファイル名
112233	映画A	0123456789..	movieA.mpg
234567	音楽B	7361278168..	musicB.wav

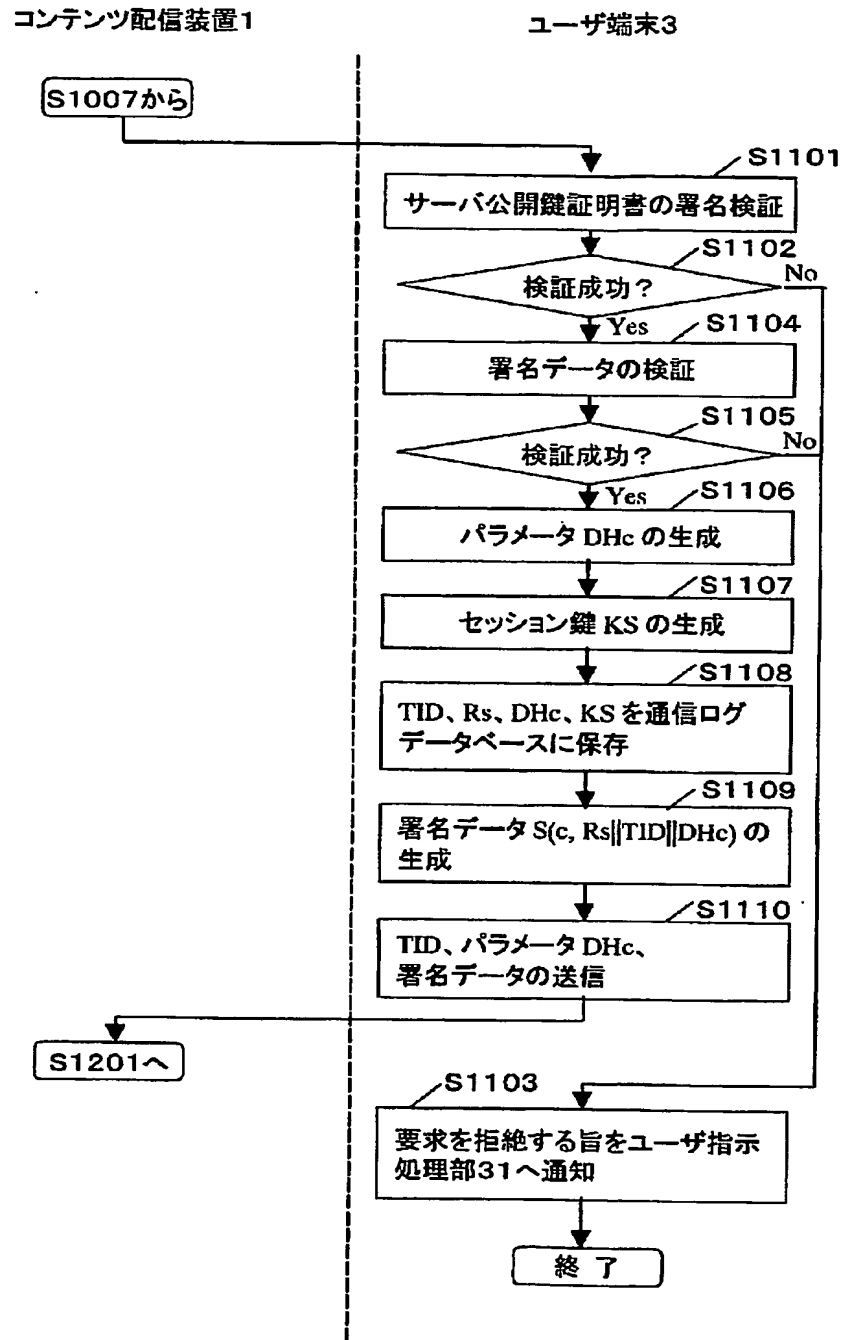
【図 9】



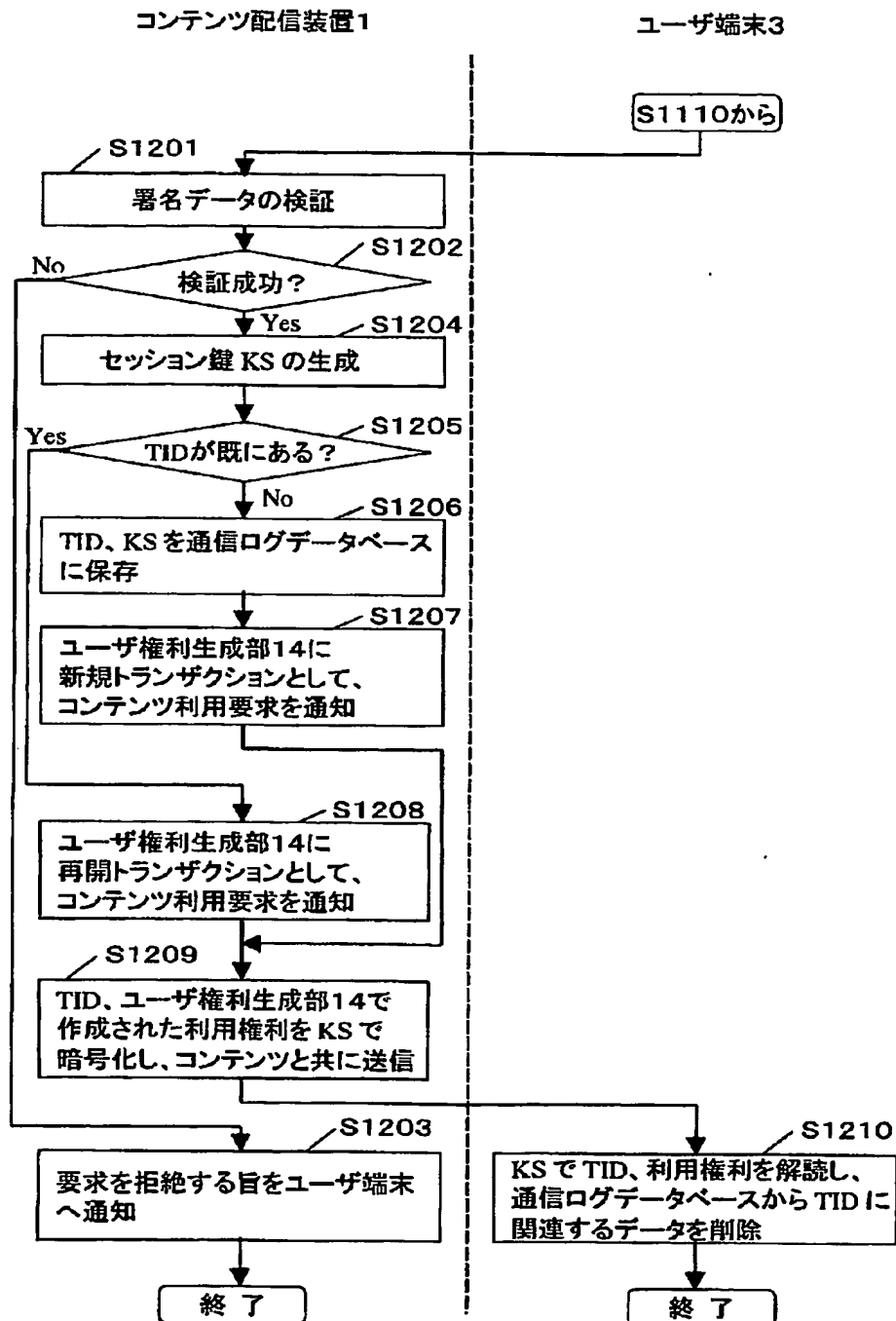
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 SACプロトコルや通信切断対策プロトコルの双方を利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となるという課題があった。

【解決手段】 サーバ装置および端末装置間の通信に、少なくとも前記サーバ装置による前記端末装置の正当性の認証と通信暗号鍵の共有を行う認証フェーズを含み、前記認証フェーズには、前記サーバ装置と前記端末装置間で通信されるトランザクションを識別する情報を交換するトランザクション識別情報交換フェーズと、前記トランザクションにおける前記端末装置からの先頭のコマンドを送信する先頭コマンド送信フェーズとを含むことにより、ユーザに対する応答時間を削減する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 1 7 6 3 7
受付番号	5 0 3 0 0 1 2 4 4 5 7
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 1 月 2 8 日

< 認定情報・付加情報 >

【提出日】	平成15年 1月27日
-------	-------------

次頁無

特願 2 0 0 3 - 0 1 7 6 3 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社